PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06F 1/00

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/12088**

(43) Internationales Veröffentlichungsdatum: 11. März 1999 (11.03.99)

(21) Internationales Aktenzeichen: PCT/DE98/02517

(22) Internationales Anmeldedatum: 27. August 1998 (27.08.98)

(30) Prioritätsdaten:
197 38 325.4 2. September 1997 (02.09.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS NIXDORF INFORMATIONSSYSTEME AG [DE/DE]; Heinz-Nixdorf-Ring 1, D-33106 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: WIEHLER, Gerhard [DE/DE]; Am Bogen 43, D-82223 Eichenau (DE).

(74) Gemeinsamer Vertreter: SIEMENS NIXDORF INFORMATIONSSYSTEME AG; Epping, Wilhelm, Postfach 22 13 17, D-80503 München (DE).

(81) Bestimmungsstaaten: AU, CA, CN, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

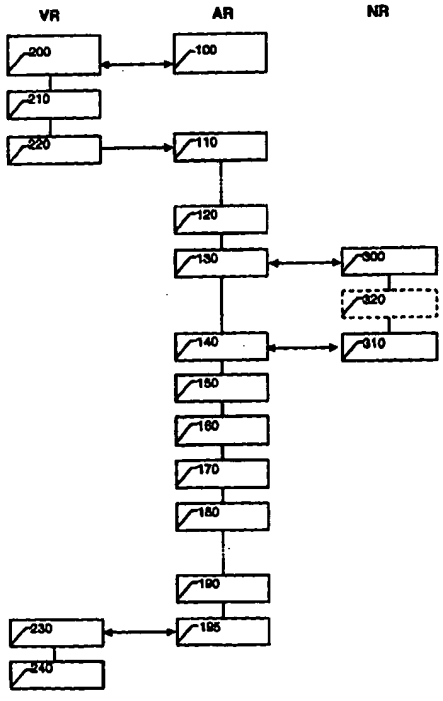
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR CONTROLLING DISTRIBUTION AND USE OF SOFTWARE PRODUCTS WITH NETWORK-CONNECTED COMPUTERS

(54) Bezeichnung: VERFAHREN ZUR STEUERUNG DER VERTEILUNG UND NUTZUNG VON SOFTWARE-OBJEKTEN BEI VERNETZTEN RECHNERN

(57) Abstract

The distribution is controlled by means of central certificates acting as a link between the authorizations granted to various users and the right-of-access code allocated to the software products in connection with a special separated control program. The certificates are issued to users on request and intended for calling the wanted software products. Such certificates can be supplemented with distinct control functions. Said functions are executed by the control program, which is supplemented accordingly, especially for recording data on the utilization volume. The invention also relates to the following items: key safety, use of a chip card, integrated copy protection.



(57) Zusammenfassung

Die Verteilung wird durch zentrale Zertifikate als Bindeglied zwischen den den einzelnen Nutzern zugeteilten Berechtigungen und den den Software-Objekten zugeordneten Berechtigungskennzeichen in Verbindung mit einem gesonderten Steuerprogramm gesteuert. Die Zertifikate werden den Nutzern auf Anforderung zugestellt und dienen zum Abruf der gewünschten Software-Objekte. Zertifikate können durch gesonderte Steuerfunktionen ergänzt werden, die vom entsprechend ergänzten Steuerprogramm ausgeführt werden, so zum Beispiel für eine Erfassung von Daten über den Nutzungsumfang. Weiterhin: Sicherung über Schlüssel, Verwendung einer Chipkarte, integrierter Kopierschutz.

REF. 3 PCA 88813
COUNTRY China
CORRES. US/UK

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Beschreibung

Verfahren zur Steuerung der Verteilung und Nutzung von Software-Objekten bei vernetzten Rechnern

Die Erfindung betrifft ein Verfahren für Datennetze, bei denen Datensammlungen oder Programme als Software-Objekte an zentraler Stelle verwaltet und auf Anforderung von mit dem Datennetz gekoppelten Rechnern über das Datennetz vorübergehend dem jeweils anfordernden Rechner zur Nutzung zur Verfügung gestellt werden, wobei die Nutzung an den Nutzern zugeteilte Berechtigungen gekoppelt ist.

Über Datennetze können Datenbänke angesteuert und dortige Datensammlungen abgefragt werden. Auch Programme können über Datentnetze den angeschlossenen Rechnern auf Anforderung zur Verfügung gestellt werden. In beiden Fällen bietet die zentrale Verwaltung derartiger Software-Objekte den Vorteil, daß immer der neueste Informationsstand oder die neueste Programmversion verfügbar ist. Der Zugriff ist meistens an entsprechende Berechtigungen gebunden, die mit Bezug auf die einzelnen Software-Objekte sehr unterschiedlich sein können. Auch sind für die Nutzung der Software-Objekte vielfach Gebühren zu entrichten, so daß eine Erfassung des Nutzungsumfanges notwendig ist.

Aufgabe der Erfindung ist es, die in Verbindung mit einer zentralen Verwaltung von Software-Objekten gegebenen Probleme der Zugangsberechtigung und der Nutzungserfassung günstig zu lösen und dabei im gesamten Datennetz eine einheitliche und flexibel anpaßbare Verteilung und Nutzung zu ermöglichen, die den verschiedensten Anforderungen gerecht wird.

Ausgangspunkt für eine derartige Lösung ist das durch die Merkmale des Patentanspruches 1 gekennzeichnete Verfahren. Danach wird der Zugang zu den Software-Objekten durch zentral erstellte, benutzerspezifische Zertifikate in Verbindung mit

einem gesonderten Steuerprogramm geregelt. Durch die damit gegebene zentrale Verwaltung der Nutzungsrechte kann sehr flexibel auf Änderungen von Zugriffsrechten der Nutzer reagiert und netzweit ein einheitlicher Verteilungsmechanismus verwendet werden.

Die Zertifikate und das gesonderte Steuerprogramm eröffnen außerdem die Möglichkeit, weitere Funktionen in einheitlicher Weise zu realisieren, indem diese durch weitere Steuerparameter bzw. entsprechende Programmfunktionen ergänzt werden. So kann entsprechend einer Weiterbildung während eines Programmlaufs ein weiteres Software-Objekt automatisch angefordert und nachgeladen werden, wenn sich eines der vorliegenden Zertifikate auf dieses weitere Software-Objekt bezieht.

Weiterhin in einfacher Weise durch das ergänzte gesonderte Steuerprogramm die Erfassung des Nutzungsumfanges abhängig von entsprechenden Angaben im Zertifikat gesteuert werden, wobei verschiedene Möglichkeiten der Erfassung gegeben sind.

Eine weitere vorteilhafte Ausgestaltung ergibt sich durch die Meldung der Daten über die Nutzungserfassung an eine zentrale Verwaltungsinstanz im Netz, so daß jederzeit Auskunft über die eingesetzten Software-Objekte und deren Nutzungsumfang gegeben werden kann. Der Zeitpunkt und der Umfang der Meldung kann unterschiedlich so gestaltet werden, daß die Rückmeldung nach Ablauf der Gültigkeitsdauer eines Zertifikats erfolgt und die zu diesem gehörigen objektbezogenen Erfassungsdaten umfaßt oder die Rückmeldung nach Ablauf der Gültigkeitsdauer für das gesonderte Steuerprogramm erfolgt und alle vorliegenden Erfassungsdaten umfaßt.

Das Verfahren kann auch auf Netze mit mehreren eigenständigen Verwaltungsinstanzen für Software-Objekte ausgedehnt werden.

Ein weiterer Vorteil besteht darin, daß das Verfahren mit verschiedenen Sicherheitsstandards arbeiten kann. Zweckmäßig

ist es, wenn alle Verbindungsherstellungen im Datennetz und Übertragungen durch Schlüssel gesichert erfolgen, die zweckmäßig auf einer benutzerbezogenen Chipkarte gespeichert sind. Die Verwendung einer Chipkarte als Datenträger bindet den Nutzer auch nicht an einen lokalen Arbeitsplatz, er kann vielmehr von jedem Rechner im Netz aus tätig werden. Dabei wird die Chipkarte zweckmäßig auch für die Erfassung der Daten über den Nutzungsumfang verwendet.

Weiterhin kann der Kopierschutz von Software-Objekten in einfacher Weise durch entsprechende Ergänzung der zugehörigen Zertifikate und des gesonderten Steuerprogramms sichergestellt werden.

Weiterhin kann der das Steuerprogramm überprüfen, ob angeforderte Software-Objekte bereits auf dem anfordernden Rechner verfügbar ist und bei positivem Ergebnis die lokale Bereitstellung des Software-Objektes veranlassen. Die mehrmalige Übertragung des Software-Objekte zum Rechner kann so unterbleiben und die Performance erhöht werden.

Insgesamt ermöglicht die Erfindung bei zentraler Software- und Rechte-Verwaltung eine dezentrale Software-Nutzung. Sie basiert auf Technologien, welche skalierbare Sicherheit gewährleisten und höchste Sicherheitsanforderungen erfüllen können. Auch löst die Erfindung die Verteilung und Nutzungserfassung gültiger Software-Versionen sowie die Löschung nicht mehr benötigter Versionen weitgehend automatisch. Eine Auskunft über die eingesetzten Software-Objekte sowie über ihre Nutzung ist jederzeit möglich. Eine netzweite Erfassung der Daten über den Nutzungsumfang kann periodisch durchgeführt werden und ist parametrisierbar, z. B. monatlich. Nutzer können Software auf beliebige am Netz angeschlossene Rechner laden und anwenden. Eine zentrale Verwaltung ermöglicht die netzweite Einhaltung von Verteilungs- und Nutzungsregeln. Gleichwohl kann dem Nutzer die Freiheit gewährt wer-

den, Einstellungen entsprechend der individuellen Gegebenheiten seines Arbeitsplatzes vorzunehmen.

Einzelheiten der Erfindung seien nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert. Im einzelnen zeigen

FIG 1 ein Übersichtsschema der für die Durchführung des Verfahrens gemäß der Erfindung benötigten Netzwerkkomponenten,

FIG 2 eine schematische Darstellung einer mit verschiedenen Schlüsseln und Programmen geladenen Chipkarte und

FIG 3 ein Ablaufdiagramm des Verfahrens gemäß derErfindung.

FIG 1 zeigt ein Netzwerk mit beispielsweise einem von mehreren Arbeitsplatzrechnern AR, der zur Nutzung aus dem Netz geladener Software verwendet wird, einer Chipkarte 10, die ein Nutzer zur Authentisierung und zum Nachweis entsprechender Software-Nutzungsberechtigungen verwendet, einem zentralen Verwaltungsrechner VR, auf dem sämtliche Software-Objekte und Software-Nutzungsberechtigungen administriert werden, und einem beliebigen Netzrechner NR , auf dem Software-Objekte gespeichert sind, die bei Anforderung auf den Arbeitsplatzrechner AR geladen werden können. Die Rechner sind über ein übliches Datenkommunikationsnetz 30 - zweckmäßigerweise über ein Internet oder Intranet - miteinander verbunden. Verwaltungsrechner VR und Netzrechner NR sind zwar logisch getrennt dargestellt, sie können aber auf derselben Hardwareplattform installiert sein.

Der Verwaltungsrechner VR enthält z. B. ein Software-Administrationsprogramm 41, im folgenden SOA-Programm genannt, ein Programm zur Erfassung der Software-Nutzungsdaten 42, im folgenden SUC-Programm genannt, ein Programm zur Administration der Software Nutzungsrechte sämtlicher Nutzer im Netz 43, im folgenden USAR-Programm genannt, und ein Programm

zur Ausstellung von Zertifikaten zum Zwecke der Software-Nutzung 44, im folgenden ISC-Programm genannt.

Das SOA-Programm 41 kann auf existierenden Produkten, z. B. SMS von Microsoft, basieren, die aber gegebenenfalls erweitert werden müssen. Es administriert eine Datenbank 45 der im Netz verfügbaren Software-Objekte. In der Software-Objekt-Datenbank werden relevante Informationen und Eigenschaften der einzelnen Objekte geführt ,z. B. Hersteller, Versions-Nr., Größe, Location im Netz, Kopierschutz,usw. In dieser oder in einer separaten Datenbank wird je Objekt ein Rollenkennzeichen geführt, das angibt, welchen Rollen im Unternehmen Zugriff auf das jeweilige Software-Objekt erlaubt ist. Typische Rollen im Unternehmen können z. B. sein: Software-Engineer, Marketing-Direktor, Executive-Manager. Der Inhalt der Software-Objekt-Datenbank kann z. B. nach den Spezifikationen des Security Modells von Microsoft vorgenommen werden.

Das SUC-Programm 42 führt in einer Datenbank 46 dynamisch die Software-Nutzungsdaten, d.h. den aktuellen Stand der auf allen Arbeitsplatzrechnern AR genutzten Software. Aktuelle Daten können hier jederzeit abgefragt werden.

Mittels des USAR-Programms 43 werden in einer Datenbank 47 die relevanten Rollen sowie die Zuordnung zu sämtlichen Nutzern im Netz definiert und verwaltet. Jedem Nutzer können eine oder mehrere Rollen zugewiesen werden. Die Anzahl der Rollen ist beliebig erweiterbar.

Das ISC-Programm 44 stellt den Nutzern auf Anforderung sogenannte „User Software Certificates" USC zur Verfügung, durch welche die Berechtigung zur Nutzung von Software erteilt wird. Zur Ausstellung der Zertifikate USC benötigt das ISC-Programm 44 Zugriff auf die Datenbänke 47 und 45.

Die Kommunikation zwischen dem Verwaltungsrechner VR und den Arbeitsplatzrechnern erfolgt zweckmäßigerweise über einen

WWW-fähigen Server 48, z. B. Microsofts Internet Information Server oder Netscape's Internet Server. Die Programme 41, 42, 43, und 44 können beispielsweise als Backend-Applikationen über sogenannte CGI-Scripts angebunden sein.

Das Administrator-Interface zur Administration der SOA- und USAR-Programme 41 und 43 bzw. das Recherche-Interface für das SUC-Programm 42 kann z. B. ein beliebig im Netz lokalisierter Browser 60 sein.

Auf dem Arbeitsplatzrechner AR ist zweckmäßigerweise ein weiterer Browser 21 installiert, welcher die Kommunikation mit den Rechnern VR und NR abwickelt. Die Software-Komponente 22, im folgenden SCV-Programm genannt, wird bei jeder Anfrage des Arbeitsplatzrechners AR auf Zuteilung von Software-Nutzungsrechten zusammen mit einer sogenannten HTML-Page zweckmäßigerweise mittels Protokoll HTTPS, z. B. als ActiveX Control oder als „Plug in", vom Verwaltungsrechner VR zum Arbeitsplatzrechner AR übertragen. Die HTML-Page stellt als Liste ASL am Bildschirm die erlaubten Zugriffsmöglichkeiten auf Netz-Software dar.

Bei einer Download-Anforderung verifiziert das SCV-Programm mittels der Zertifikate USC die Nutzungs-Berechtigung. Das SCV-Programm steuert desweiteren die Erfassung der Software-Nutzungsdaten, z. B. Anzahl der Downloads, Nutzungszeit einer SW,usw..

Die Programme 24 bis 2x sind z. B. Anwendungsprogramme, die der Nutzer aus dem Netz geladen hat und anwendet.

Die Chipkarte 10 wird über einen üblichen, am Arbeitsplatzrechner AR angeschlossenen Chipkartenleser 23 betrieben. Die Karte entspricht zweckmäßigerweise dem Standard 7816. Vorteilhafter ist aus Sicherheitsgründen eine Chipkarte mit Cryptocontroller, wie z. B. SLE 44CR80S von Siemens, da diese

für offene Netze, wie z. B. das Internet mit auf Public Key-Basis arbeitenden Sicherheitsmechanismen, besonders geeignet.

Chipkartenanwendungen und Chipkartenleser können z. B. im Arbeitsplatzrechner AR entsprechend den von der „PC/SC Workgroup" festgelegten Spezifikationen und Interfaces, unterstützt werden. Weitere Information dazu sind unter

http://www.smartcardsys.com.

zu finden.

Jeder Nutzer am Netz erhält eine individuelle Chipkarte. Die Chipkarte wird vor Auslieferung an den Nutzer in einem sogenannten Personalisierungsprozeß, z. B. bei einem Kartenhersteller, mit den persönlichen Daten des Nutzers personalisiert. Mindestens müssen, wie FIG 2 zeigt, ein privater Schlüssel 11a und ein Zertifikat des öffentlichen Schlüssels 11b des Nutzers auf die Karte gespeichert (personalisiert) werden. Der private Schlüssel und das Zertifikat des öffentlichen Schlüssels des Nutzers werden z. B. in einem Trust Center erzeugt und auf sicherem Wege der Personalisierungsstelle zur Verfügung gestellt, wo sie dann in üblichen Verfahren auf die Chipkarte gespeichert werden.

Mittels dieses Schlüssel-Zertifikatspaares 11a/11b und eines entsprechenden Paares auf dem Verwaltungsrechner VR kann nach heute üblichen Verfahren, z. B. SSL V3.0, eine beidseitige und sichere Client/Server-Authentisierung durchgeführt werden. Dies ist die Voraussetzung für die sichere Übertragung von Zertifikaten USC, die der Nutzer zur Nutzung von Software benötigt.

Je nach Sicherheitsanforderungen können weitere Schlüssel-Zertifikatspaare 12a/12b - z. B. für einen Intergritätsschutz von Zertifikaten USC oder die sichere Kommunikation zwischen Programmen auf dem Verwaltungsrechner VR und dem Arbeitsrech-

ner AR oder für das Nachladen von Schlüsseln oder Anwendungen auf die Karte über das Netz - auf die Chipkarte personalisiert bzw. im Netzbetrieb nachträglich mittels sicherer Verfahren auf die Chipkarte geladen werden.

Bereits bei der Personalisierung oder ebenfalls im Netzbetrieb werden Applikationsprogramme 13a bis 13x auf die Chipkarte geladen, die der Erfassung der Software-Nutzung, z. B. Anzahl der Downloads oder Zeiterfassung, dienen.

Anhand von FIG 3 wird das Verfahren des Software-Downloads, der Software-Nutzung und der Nutzungserfassung erläutert. Folgende Verfahrensschritte werden dabei ausgeführt:

100: Der Nutzer meldet sich beim Verwaltungsrechner VR an und authentisiert sich mittels des üblichen HTTPS-Protokoll im SSL-Dialog unter Verwendung seines privaten Schlüssels auf der Chipkarte.

200: Der Verwaltungsrechner VR authentisiert sich ebenfalls und identifiziert den Nutzer.

210: Der Verwaltungsrechner VR stellt unter Auswertung der Datenbänke 45 und 47 die Inhalte der nutzerspezifischen Zertifikate USC bereit.Dabei werden Zertifikate für jene Software-Objekte erstellt, deren Rollenkennzeichen mit einer oder mehreren Rollen, die der Nutzer besitzt, übereinstimmt.
Ein Zertifikat USC kann z. B. enthalten: Software-ID, Versions-Nr., Location im Netz, Größe des Software-Objekts, Art der Nutzungserfassung, Zeitintervall der Erfassungsmeldung an den VR, Löschungsmodus, Gültigkeitsdauer des USC, ID des ausstellenden Verwaltungsrechners VR.
Bei der Art der Nutzungserfassung können z. B. folgende Parameter Verwendung finden: Erfassung der Download-Anzahl, Erfassung der aktiven Nutzungszeit, keine Erfassung.

220: Die bereitgestellten Zertifikate USC werden mit dem Public Key des Nutzers im Verwaltungsrechner VR integritätsgeschützt, gegebenenfalls auch zusätzlich mit im Internet üblichen Verfahren verschlüsselt,) und eingebunden in die HTML-Page ASL zusammen mit dem SCV-Programm 22 an den Arbeitsplatzrechner AR übertragen.
Da das SCV-Programm im Arbeitsplatzrechner AR sicherheitsrelevante Funktionen ausführt, sollte es zweckmäßig mit einer digitalen Signatur des Verwaltungsrechner VR versehen sein.

110: Im Arbeitsplatzrechner AR erscheint die HTML-Page ASL auf dem Bildschirm. Sie zeigt alle dem Nutzer zugänglichen Software-Objekte an.
Implizit ist eine Gültigkeitsdauer in der HTML-Page enthalten, nach deren Ablauf sich die Page samt des SCV-Programm und der Zertifikate USC zerstören. Für die Dauer der Gültigkeit wird sie im Browser verfügbar gehalten und kann nach jedem Einschalten des Arbeitsplatzrechners AR ohne Kommunikation mit dem Verwaltungsrechner VR aufgerufen werden. Nach jedem Aufruf des SCV-Programms kann vorzugsweise eine Verifikation der digitalen Signatur erfolgen, um Manipulationen zu vermeiden bzw. zu entdecken.

120: Der Nutzer kann nun die zum Download gewünschten Software-Objekte anklicken. Dadurch wird automatisch das SCV-Programm gestartet. Das SCV-Programm und die betreffenden Zertifikate USC werden daraufhin unter Verwendung der auf der Chipkarte befindlichen Schlüssel verifiziert.

130: Nach positiver Verifizierung ermittelt das SCV-Programm die Netzrechner-Adresse(n) aus dem(n) Zertifikaten USC und stellt die WWW-Verbindung zum ersten Netzrechner NR her. (Nach abgeschlossenem Download gegebenenfalls auch zu weiteren Netzrechnern NR.)

130/300: Es erfolgt die gegenseitige Authentisierung zwischen Arbeitsplatzrechner AR und Netzrechner NR entsprechend einem üblichem Verfahren.

310/140: Danach kann das Programm 51 das (die) gewünschte(n) Software-Objekt(e) selektieren und an den Arbeitsplatzrechner AR senden.

320: Zur Erhöhung der Sicherheit, insbesondere bei Anwendung des Verfahrens im Internet, kann es sinnvoll sein, im Netzrechner NR ebenfalls eine Verifizierung der Zertifikate USC mittels des Programms 53 nach üblichen Verfahren vorzunehmen. Beispielsweise werden die Zertifikate USC im Arbeitsplatzrechner AR mit dem Private Key des Nutzers signiert und im Netzrechner NR mit seinem Public Key verifiziert. In diesem Fall würde die Freigabe des angeforderten Software-Objekts aus der Objektdatenbank 52 erst nach positiver Verifikation erfolgen, wie gestrichelt angedeutet.

Eine weitere Erhöhung der Sicherheit kann dadurch erreicht werden, daß das zu übertragende Software-Objekt im Netzrechner NR mit einer digitalen Signatur versehen wird und im Arbeitsplatzrechner AR vor Nutzung eine Verifikation erfolgt. Damit könnte eine Verfälschung des Objektes bei der Netzübertragung entdeckt werden.

150: Im nächsten Schritt stellt auf dem Arbeitsplatzrechner AR das SCV-Programm 22 anhand der USC-Parameter die Art der Nutzungserfassung fest und wird entsprechend tätig. Beispielsweise wird, wenn der Parameter „Erfassung der Anzahl von Downloads" gesetzt ist, eine objektbezogene Zähleranwendung auf der Chipkarte, z. B. 13a in FIG 2, aktiviert und der Zähler erhöht. Zählvorgänge auf der Chipkarte werden zweckmäßig in üblicher Weise kryptographisch abgesichert durchgeführt.

160: Der Nutzer erkennt nach dem Download an Hand der Liste ASL auf dem Bildschirm, welche Software lokal vorhanden ist, und kann den Start per Klick auslösen.

170: Dadurch wird gleichzeitig - falls ein dementsprechender USC-Parameter gesetzt ist - die Nutzungszeiterfassung durch das SCV ausgelöst und die Nutzungszeit während der aktiven Nutzung periodisch erfaßt, indem das SCV-Programm 22 einen objektbezogenen Zeitzähler auf der

Chipkarte, z. B. 13b in FIG 2, von Zeit zu Zeit (parametrisierbar) erhöht.

180: Nach Beendigung der Nutzung eines geladenen Software-Objektes auf dem Arbeitsplatzrechner AR entscheidet das SCV-Programm 22 anhand des Löschungsmodus-Parameters, ob das Programm gelöscht oder im Arbeitsplatzrechner AR gespeichert wird.

190: Eine Nutzungserfassungs-Rückmeldung an den VR wird entweder durch Ablauf des Zeitintervall-Parameters eines Zertifikats USC oder durch Ablauf eines Zeitintervalls im SCV-Programm 22 ausgelöst. Im Falle der Zertifikats-Auslösung sind nur die zum betreffenden Zertifikat USC gehörenden objektbezogenen Erfassungsdaten betroffen, im SCV-Auslösungsfall die Erfassungsdaten sämtlicher Zertifikate USC. Entsprechend werden die zugehörigen Download-Zähler und Nutzungszeitzähler aus der Chipkarte 10 ausgewählt.

195/230: Nach der üblichen gegenseitigen Authentisierung zwischen Arbeitsplatzrechner AR und Verwaltungsrechner VR werden die ausgewählten Zählerstände an den Verwaltungsrechner VRübertragen.

240: Im Verwaltungsrechner VR werden die entsprechenden Erfassungsdaten mittels des SUC-Programms 42 ausgewertet und in die Datenbank 46 eingetragen.

Bei Ziehen der Chipkarte erscheint z. B. eine Dialogbox mit der Warnung, daß das Programm nach einer bestimmten Zeit (parametrisierbar) gelöscht wird, wenn die Karte nicht wieder eingeführt wird.

Das beschriebene Verfahren ermöglicht durch die zentrale Verwaltung der Nutzungsrechte und Nutzungserfassungsparameter im Verwaltungsrechner VR eine netzweit einheitliche und flexibel anpaßbare Software-Verteilung und -Nutzung. Gleichwohl kann der Nutzer einzelne Parameter ändern oder selbst bestimmen, falls ein entsprechender USC-Parameter diesen Freiheitsgrad

erlaubt. Z. B. kann der Nutzer das Löschen oder Speichern eines Programms nach Nutzung selbst entscheiden.

Im Falle der Änderung einzelner USC-Parameter durch den Nutzer bleibt das ursprünglich integritätsgeschützte Zertifikat USC unverändert, wodurch gewährleistet wird, daß bei wiederholten Downloads jeweils eine Integritäts-Verifikation durchgeführt werden kann.

Die Funktionalität kann dadurch erweitert werden, daß ein automatischer Download durch das SCV-Programm 22 für den Fall ausgelöst wird, wenn ein Software-Objekt zur Laufzeit ein anderes Software-Objekt aufruft, z. B. OLE-Technik, das nicht auf dem Arbeitsplatzrechner AR verfügbar ist, dessen Identität aber in einem der Zertifikate USC festgestellt werden kann.

Der Nutzer in einem Netzwerk kann das Verfahren von beliebigen am Netz angeschlossenen Rechnern aus anwenden, wenn er jeweils seine individuelle Berechtigungs- und Erfassungs-Chipkarte an diesem Rechner betreiben kann. Bei einem Rechnerwechsel muß er lediglich vor dem ersten Download eines Software-Objektes mit dem Verwaltungsrechner VR kommunizieren, um sich die aktuellen Rechte entsprechend dem oben beschriebenen Verfahren erteilen zu lassen.

Bei fortschreitender Chipkarten-Technologie kann die HTML-Page mit der Liste ASL und das SCV-Programm auf der Chipkarte gespeichert sein und zum Ablauf gebracht werden. In diesem Fall entfällt bei Rechnerwechsel die Kommunikation mit dem VR.

Aus Sicht des Nutzers läßt sich das Verfahren auch auf verschiedene, voneinander unabhängige Netze anwenden, z. B. Intranet für Rechte innerhalb der eigenen Firma, Extranet für Rechner in einer Partnerfirma, Internet für Rechte zur welt-

weiten Nutzung. Das kann mit ein und derselben oder mit separaten Chipkarten erfolgen. Bei Verwendung derselben Chipkarte müssen separate Schlüssel für die verschiedenen Verwaltungsrechner VR zur Verfügung stehen.

Eine Erweiterung des Verfahrens ist auch dadurch möglich, daß Mechanismen zum Kopierschutz in das beschriebene Verfahren einbezogen werden. Hierzu wird für Software-Objekte, die kopiergeschützt sein sollen, unter Verwendung des Public Key des Nutzers eine sog. „Key File" erzeugt, die der Nutzer nach dem Download des Software-Objekts erhält. Nur mit dieser „Key File" und unter Verwendung des Private Key des Nutzers kann das Software-Objekt genutzt werden.

Durch Festlegung eines USC-Parameters „kopiergeschützt" und Erweiterung der Funktionen des SCV-Programms für die erforderliche Kommunikation zwischen Arbeitsplatzrechner AR und Verwaltungsrechner NR sowie Arbeitsplatzrechner AR und Chipkarte 10 entsprechend der für den Kopierschutz festgelegten Verfahren, läßt sich der Kopierschutz einfach in das hier erläuterte Verfahren integrieren.

Für das Verfahren können außerdem multifunktionale Chipkarten verwendet werden, die z. B. auch für andere Netzanwendungen eingesetzt werden. Vorzugsweise ist eine Kombination mit Anwendungen zur Identifikation im Netz sinnvoll. Solche Anwendungen könnten z. B. sein: WWW-Client Authentifikation gegenüber einem Internet Server, WWW-Client Identifikation bei Mail (z. B. S/MIME), WWW-Client Identifikation zur Gewährung von Zugriffsrechten auf Netzressourcen.

Das Verfahren kann generell auch - bei geringeren Sicherheitsanforderungen - ohne die Verwendung von Chipkarten angewandt werden. Die auf der Chipkarte befindlichen Schlüssel und Zähler können z. B. auch auf einer Diskette (z. B. mit einem Paßwort verschlüsselt) geführt werden, und die auf der

Chipkarte durchgeführten Operationen könnte das SCV-Programm 22 übernehmen.

5

Patentansprüche

1. Verfahren zur Steuerung der Verteilung und Nutzung von als Software-Objekte bezeichnete Datensammlungen oder Programme bei über ein Datennetz (30) gekoppelten Rechnern (AR) an zentraler Stelle (NR) verwaltet und auf Anforderung vorübergehend dem jeweils anfordernden Rechner (AR) zur Nutzung zur Verfügung gestellt werden, wobei

- die Nutzungsrechte in Form von benutzerspezifischen Zertifikaten (USC) ausgebildet sind, die als Bindeglied zwischen den den einzelnen Benutzern zugeteilten Berechtigungen und den Software-Objekten zugeordneten Berechtigungskennzeichen erstellt werden;
- bei jeder Anfrage nach einem Software-Objekt an eine zentrale Verwaltungsinstanz (VR) die Zertifikate (USC) jeweils nutzerbezogen an den anfordernden Rechner (AR) übertragen werden;
- die Zertifikate (USC) vor der Nutzung der Software-Objekte mittels eines persönlichen Datenträgers (10) verifiziert werden und die Nutzung auf dem selben Datenträger (10) erfaßt wird;
- ein gesondertertes Steuerprogramm (SCV-Programm 22) im anfordernden Rechnern (AR) auf Basis der Nutzungsrechte die das Software-Objekt betreffenden Aktionen steuert und Statusmeldungen an die zentrale Stelle (NR) meldet.

2. Verfahren nach Anspruch 1, bei dem das Steuerprogramm (SCV) von der zentralen Stelle (NR) zum anfordernden Rechner (AR) übertragen wird und vor seiner Nutzung mittels des persönlichen Datenträgers (10) verifiziert wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem die benutzerspezifischen Zertifikate (USC) auf dem als Chipkarte ausgebildeten Datenträger (10) gespeichert werden.

4. Verfahren nach Anspruch 3, bei dem das Steuerprogramm (SCV) im Datenträger (10) residiert und zumindest teilweise dort ausgeführt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem der Datenträger (10) mit beliebigen Rechnern (AR) des Datennetz (30) gekoppelt werden kann.

6. Verfahren nach einem der Ansprüche 1 bis 5, bei dem das Steuerprogramm (SCV) überprüft ob angeforderte Software-Objekte bereits auf dem Rechner (AR) verfügbar ist und bei positivem Ergebnis die lokale Bereitstellung des Software-Objektes veranlaßt.

7. Verfahren nach einem der Ansprüche 1 bis 6, bei dem nach Übertragung der Zertifikate (USC) ein Verzeichnis der den Zertifikaten entsprechenden Software-Objekte auf dem Bildschirm des anfordernden Rechners (AR) dargestellt wird und die Anforderung für das jeweils gewünschte Software-Objekt durch den Nutzer ausgelöst wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem die Bereitstellung der Software-Objekte durch verschiedene Rechner (NR) im Netz (30) erfolgen kann.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem in den Zertifikaten (USC) enthaltene Steuerparameter durch den Nutzer änderbar sind, ohne daß ein bestehender Integritätsschutz verloren geht.

10. Verfahren nach einem der Ansprüche 1 bis 9, bei dem ein während der Laufzeit eines Programms als Software-Objekt aufgerufenes weiteres Programm, das in einem der vorliegenden Zertifikate (USC) bezeichnet ist, automatisch durch das gesonderte Steuerprogramm (22) angefordert und daraufhin an den die Anforderung stellenden Rechner (AR) übertragen wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, bei dem die Löschung von Software-Objekten automatisch bei Beendigung ihrer Nutzung erfolgt.

12. Verfahren nach einem der Ansprüche 1 bis 11, bei dem die Zertifikate (USC) Angaben über die Art der Erfassung des Nutzungsumfanges der an einen anfordernden Rechner (AR) übertragenen Software-Objekte enthalten und daß das gesonderte Steuerprogramm (22) auf Grund dieser Angaben die Erfassung des Nutzungsumfanges steuert.

13. Verfahren nach Anspruch 12, bei dem der Nutzungsumfang durch Zählung der übertragenen Software-Objekte erfolgt.

14. Verfahren nach Anspruch 12,
dadurch gekennzeichnet,
daß der Nutzungsumfang durch Zählung von periodisch wiederkehrenden Taktimpulsen erfolgt.

15. Verfahren nach einem der Ansprüche 12 bis 14, bei dem die Erfassung der Daten über den Nutzungsumfang auf dem Datenträger (10) erfolgt.

16. Verfahren nach einem der Ansprüche 1 bis 15, bei dem in Datennetzen (30) mit mehreren unabhängigen Verwaltungsinstanzen (VR) für Software-Objekte jede Verwaltungsinstanz Nutzungszertifikate (USC) für die zu ihrem Zuständigkeitsbereich gehörenden Software-Objekte erstellt.

17. Verfahren nach einem der Ansprüche 1 bis 16, bei dem alle Verbindungsherstellungen im Datennetz (30) und Übertragungen durch Schlüssel gesichert erfolgen.

18. Verfahren nach Anspruch 17, bei dem die Schlüssel auf dem Datenträger (10) enthalten sind.

19. Verfahren nach einem der Ansprüche 1 bis 18,
dadurch gekennzeichnet,
daß dem Kopierschutz unterliegende Software-Objekte durch zusätzliche Steuerparameter im zugehörigen Zertifikat (USC) und entsprechende Steuerfunktionen im gesonderten Steuerprogramm (22) gegen ein Kopieren gesichert werden.

BERICHTIGTES BLATT (REGEL 91)
ISA/EP

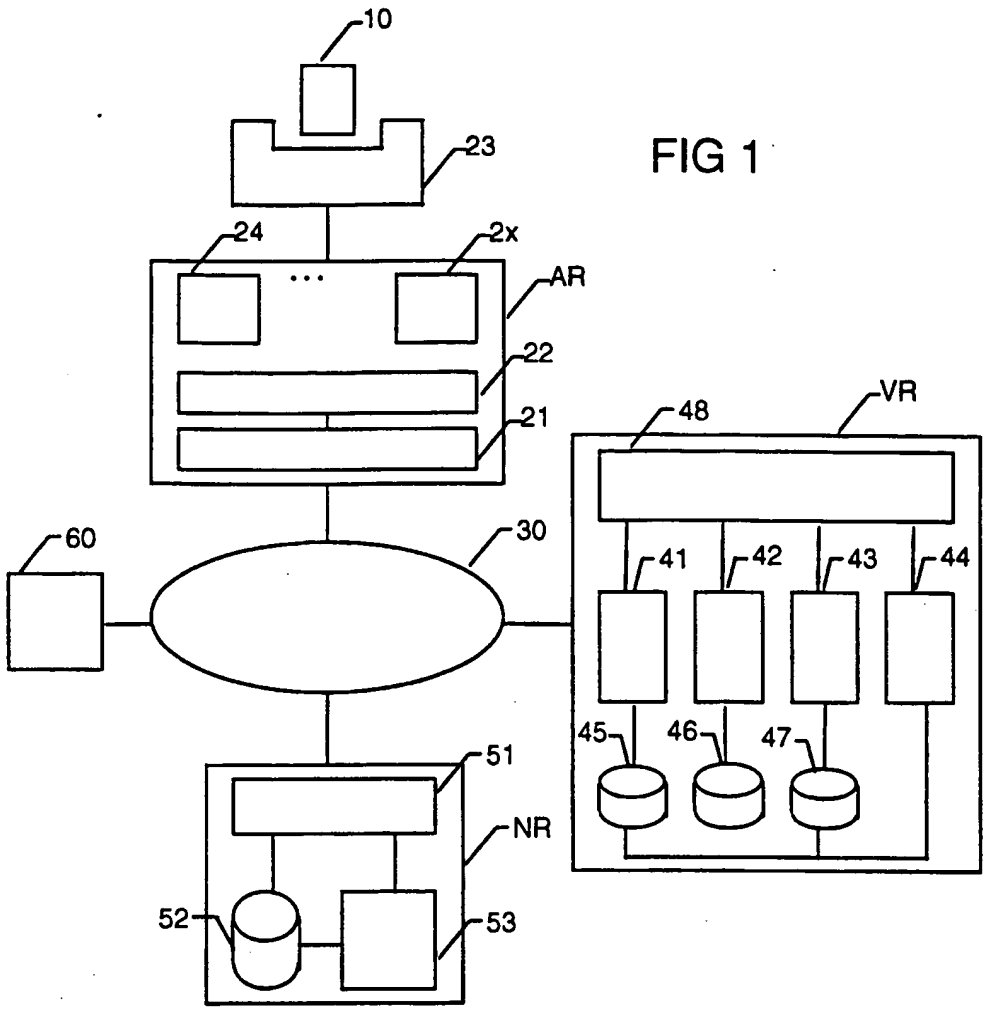

10
23
24
2x
AR
22
21
48
VR
60
30
41
42
43
44
45
46
47
51
NR
52
53

FIG 1

FIG 2

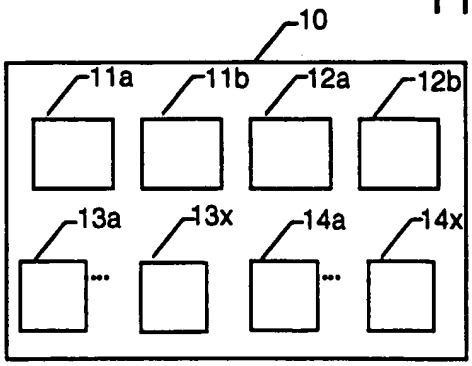
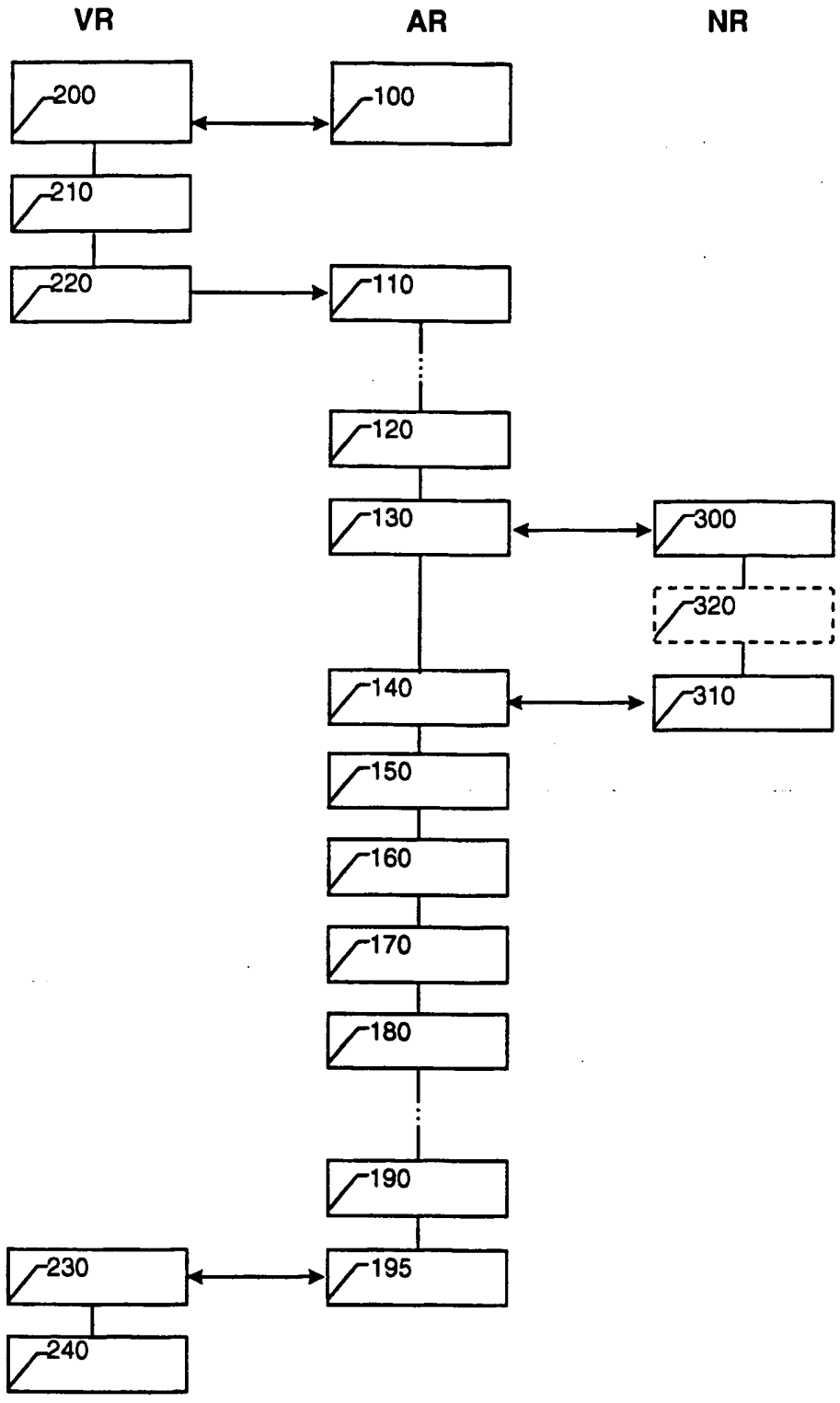

10
11a
11b
12a
12b
13a
13x
14a
14x

FIG 3


VR
AR
NR
200
100
210
220
110
120
130
300
320
140
310
150
160
170
180
190
230
195
240

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/DE 98/02517

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 421 409 A (IBM) 10 April 1991 see figures 2,5-9,13,14 see page 3, line 35 - page 4, line 29 see page 6, line 18 - page 8, line 27 see page 9, line 53 - page 11, line 26	1-9,12, 17-19
A	WO 95 05050 A (TECHNOLOGY INC B V) 16 February 1995 see figures 1,3,4,6 see page 13, line 29 - page 17, line 9 see page 18, line 35 - page 21, line 3	1,2, 6-13,16, 17,19

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 1999	25/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ational Application No
PCT/DE 98/02517

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A,C	07-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992
WO 9505050 A	16-02-1995	US 5418713 A	23-05-1995
		AU 7519994 A	28-02-1995
		CA 2192814 A	16-02-1995
		EP 0716795 A	19-06-1996
		US 5794217 A	11-08-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/02517

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 421 409 A (IBM) 10. April 1991 siehe Abbildungen 2,5-9,13,14 siehe Seite 3, Zeile 35 - Seite 4, Zeile 29 siehe Seite 6, Zeile 18 - Seite 8, Zeile 27 siehe Seite 9, Zeile 53 - Seite 11, Zeile 26 ---	1-9,12, 17-19
A	WO 95 05050 A (TECHNOLOGY INC B V) 16. Februar 1995 siehe Abbildungen 1,3,4,6 siehe Seite 13, Zeile 29 - Seite 17, Zeile 9 siehe Seite 18, Zeile 35 - Seite 21, Zeile 3 -----	1,2, 6-13,16, 17,19

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. Januar 1999	25/01/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. ..ionales Aktenzeichen
PCT/DE 98/02517

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A,C	07-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992
WO 9505050 A	16-02-1995	US 5418713 A	23-05-1995
		AU 7519994 A	28-02-1995
		CA 2192814 A	16-02-1995
		EP 0716795 A	19-06-1996
		US 5794217 A	11-08-1998